ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

Security and Privacy Challenges in Online Social Networks

[1] Deepthi Peri [2] Bhargav Sundararajan
[1][2] Department of Computer Science Engineering,
SRM University, Kattangulathur, Chennai, India

Abstract: **- With the increasing popularity of Online Social networks, the threats associated with it have also been on the rise. In this paper, we will discuss the various security and privacy challenges in Online Social Networks and also the preventive and mitigative measures to counter them. We also provide a case study on the existing authentication and security framework of Facebook. In the end, we review two possible future implementations which can help enhance the security of Online Social Networks.**

Index Terms:**—authentication, privacy, security, social networks, threats.**

I. INTRODUCTION

A social networking site[1] is an online community that is used by people to build social relations and share resources with other people who have similar personal or career interests, activities, backgrounds or real-life connections. Social networking sites are varied and are incorporated through various platforms and cater to people with different interests. Social network services can be split into three types: socializing social network sites are primarily for socializing with friends (e.g., Facebook [6]); networking social networking sites are for non-social interpersonal communication (e.g., LinkedIn [7]); and social navigation social network site enables helping users to find specific information or resources (e.g., Goodreads) With the advent of these online social networking sites the world is online. These social networking sites are hugely popular as they provide the opportunity to interact with new people across the globe and connect with old friends and family. They have taken the place of chat rooms and clubs where people with similar interests can gather and interact. Social media also has a huge share in the job market. It helps businesses reach out and advertise as well as help recruit eligible workers. Moreover, these online social networks are immensely user friendly and free to use, that their popularity comes as no surprise. As of 2016, the number of active users on Facebook was estimated at 1.86 billion users [2] and the number of Twitter [8] users were averaged at 319 million monthly users. People tend to share all kinds of personal and private information including pictures, videos, documents and their current location on these social networking sites. As a part of online profile building, users are encouraged to provide their name, contact details, employer details, schooling and college information, hobbies and special interests. This sharing of data has enabled a wide range of possible security and privacy threats [3] and has given rise to malicious attackers. These attackers use this information to carry out several planned attacks like scams, id thefts and hacking [4].

The structure of the paper is as follows. Section II discusses the various threats in social networks and how they affect the users [5]. In Section III the necessary preventive and mitigative measures are listed for those threats. Then a case study about Facebook's authentication and security framework is done in Section IV. Section V then suggests some research and future implementations to better security in social networks. A brief conclusion of this paper is provided in section VI.

II. THREATS IN SOCIAL NETWORKS

A. Identity Theft

Identity theft [12] is a fraudulent practice of misusing another person's personal information such as name, address, date of birth, relationship status, and other affiliations, interests and hobbies. Millions of people every year are affected by identity theft from social networking sites, costing them countless hours and money in identity recovery and repair. Social media sites generate revenue with targeted advertising, based on personal information. As such, they encourage registered users to provide as much information as possible. Using the available personal details of the user like name, date of birth and family details, confidential information such as social security

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

numbers, bank account details and other sensitive data can be accessed. As per the Identity Theft Resource Center (ITRC), there are five basic types of identity theft namely financial, criminal, medical, governmental, and cyber/reputational. Cyber/reputational identity theft is a recently evolved form of identity theft, thanks to increasing popularity of social media. For example, duplicate Facebook profiles have become a menace to social media users, posing as a danger to personal space and reputation. It is estimated that anywhere between 52.89 million and 97.17 million accounts are duplicates on Facebook with many of them going undetected and unreported. With limited government oversight, industry standards or incentives to educate users on security, privacy and identity protection, users are exposed to identity theft and fraud. Identity theft can lead to numerous deadly consequences. The most obvious and most dangerous is the financial loss, which can be either direct or indirect. Direct costs include the amount of money stolen or misused by the offender. On the other hand indirect financial costs are those outside costs such as legal fees or overdraft charges associated with identity theft. Apart from the financial loss, identity thefts also take a toll on the victim's emotions.

B. Click Streaming

Click streaming is the process of recording, analyzing and reporting aggregate data about which websites a user visits in cyberspace along with the order. A "clickstream" is the aggregation of the electronic information generated as a Web user communicates with other computers and networks over the Internet. This data can be shockingly revealing, providing a record of the entirety of one's online experience, including movements among Web sites, geographical location, the type of computer and Internet browser in use, and any transactions or comments made at individual Web sites. Social networking sites sell this data to advertisers who in turn mine this data to generate advertisements fabricated for one particular user. Clickstream data poses a dramatic risk to the personal privacy of the users since it can be collected, stored, and reused indefinitely. Unfortunately, most users are not aware of this massive collection of data regarding their behavior online. LinkedIn is one social website where the threat of data mining can be a threat. Cyber criminals take the bulk of the corporate information about the companies and who they employ and launch spear phishing attacks on them. In order to avoid legal allegations, most social networking sites mention this somewhere in the middle of the never ending Terms & Conditions, which the users are forced to accept in order to create an account in that site. As click streaming can be deleterious to the privacy of the user, all social networking sites much mention this explicitly and the user should be given the choice whether to accept it or not.

C. Cyber Stalking

Cyber stalking is the use of internet and social media to stalk or harass a user with the help of private information acquired from their social media profiles. It often leads to defamation, threats and identity thefts. In most cases cyber stalking does not remain virtual. Malicious stalkers with professional, monetary or sexual motives compromise the security of the victim in the real world too. A recent study revealed that approximately 63% of the Facebook profiles are visible to the public. Profiles without privacy protection are easy targets for cyber stalkers, with vulnerable private and personal data such as images and videos which can be easily acquired and misused. Users provide phone numbers and email addresses which can be used to harass them. Sites like Facebook and Twitter allow user to update their current location online, providing leeway for stalkers to physically track them.

D. Survey Scams & Clickjacking

Survey scams [11] are vicious schemes that lure users of social media into opening malicious web links. The post which contains the link comes along with a catchy tagline that entices the user into opening it. These taglines promise free gifts, valuable products and services like cruise tickets, expensive gadgets or money and require the user to complete a survey which demands personal details. Some famous survey scams include "IPhone 7 giveaway", "Amazon gift voucher giveaway" and others. This breach of private data can lead to other privacy threats like identity theft and cyber stalking. Another popular attack prevalent on social networking sites using these seemingly harmless taglines is Clickjacking. It is a user interface redress attack where an embedded code in the link "hijacks" the users system, performing some unintended harmful function. The twitter worm is a well-known Clickjacking example. This attack directed the users to retweet the link of the malicious page, sharing it all over the network.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

E. Phishing

Malicious attackers create fake websites that look exactly like the original social media login webpage. These links or attachments appear to be sent to the user by a known contact or organization, usually through email, requesting the user to login though the given link for said authentication or confirmation purposes. Once the user opens the link and attempts to login, their login credentials are recorded and stored, later to be used for unethical purposes. Some links might also install malware such as viruses, worms or Trojan horses onto the host computer. The most recent mass phishing attack, called the "Fake Facebook Friend Attack" used a similar strategy wherein the user received a notification saying that a friend mentioned him/her in a comment. When the user clicked the notification, a Trojan was downloaded, which installed a malicious chrome browser extension that recorded all passwords, credit card details and browsing data of the user. An estimated 10,000 Facebook users were reported to have been affected by this particular attack.

F. Social Spam

Social Spam involves contacting people with unwanted content or requests in social media. This includes sending bulk messages, excessively posting links or images to people's profiles, sending fraudulent invitations or appointments and sending friend requests to unknown people. As filters in email spam have become increasing efficient nowadays, less than 5 percent of the email spam only reach the recipient's inbox. Eventually, spammers had to discover an alternate path to reach the net user and the augmentation of social media came as a blessing in disguise for them. Bulk spamming is the most recent trend in social spamming. In this, messages with similar texts are posted simultaneously by numerous fake accounts which will make it trend worldwide. This will bait users in to visiting the link embedded in the post. In 2009, a similar spam attack was devised on twitter where people were tricked into clicking a link which said Google was hiring people for online jobs.

III. PREVENTIVE AND MITIGATIVE MEASURES

Now we have reviewed the various attacks in online social networks, we will discuss in this section about various preventive and mitigative countermeasures, both in perspective of the user as well as the social network provider

- User must remain cautious while posting sensitive information such as Social Security numbers, personal details, phone numbers, address etc. which can be easily misused. Once the information is online, it always remains online even if the user deletes it.
- Users should not open unknown links posted by strange pages or people, as they might breed malware. Users should beware of shortened URLs and redirected links.
- Users should read the term and conditions imposed on them while creating an account in any online social network so as to be aware of how their profiles and personal data might be used.
- Users must also be vigilant about fancy and enticing posts that promise extravagant products or services as most of them are fraudulent.
- Users must make sure their antivirus software is up to date so as to protect their PC from malware.
- Users must report any suspicious posts or profiles they come across on the network.
- Every social network will provide users with sufficient privacy and account security settings. Users should make ample use of these settings to ensure highest level of protection.
- Social networks should also install malware detection filters for scanning third party links posted by users on the network.
- Social network credential databases must be given the highest level of security in order to prevent mass data breaches.
- Private messages sent between users must be encrypted during transmission so as to avoid eavesdropping and Man in The Middle attacks.

IV. A CASE STUDY ON FACEBOOK'S SECURITY

A. Authentication and Security Frameworks

Facebook is home to approximately 1.86 billion monthly active users. This is almost 3 times the number

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

compared to its closest competitor, Instagram [9]. Being the most widely used social network, it is also the most vulnerable [10]. Hence it is important for Facebook to have a robust security framework. In this section we provide a case study on the existing authentication and security models in Facebook.

Figure 1 depicts the structure of Facebook Authentication Framework. In order to login, the user enters the Secure Facebook URL. The user is now redirected to the login page of Facebook. In the login page, the user is requested to enter his username and password. Facebook then checks if the entered credentials match. If they match, the user successfully logs into his/her account. If they do not match even after several attempts, a One Time Password (OTP) is sent to the registered trusted contact of the user. The user must them contact his/her trusted contact and acquire the OTP in order to login. If all the above steps fail, then the account of the user is locked and an email notification is sent to the user. Another method in which a user can login if he/she forgot the password is through Profile Picture Login. In this authentication method, Facebook with the an algorithm, displays the profile pictures of some of the closest friends friends of the user and requests the user to identify them. If the user is successfully able to identify them, then he/she will be able to reset the password and login to the account.

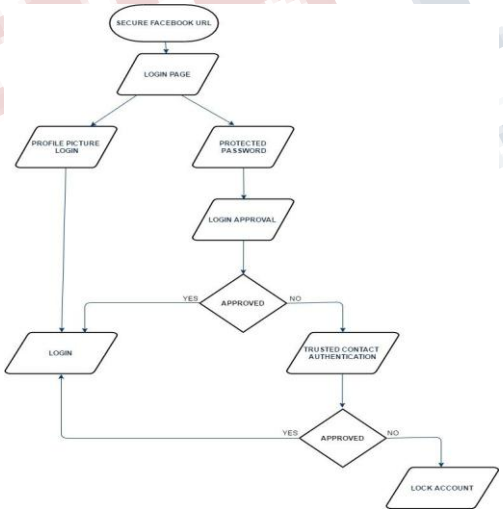

Fig. 1. Facebook Authentication Framework

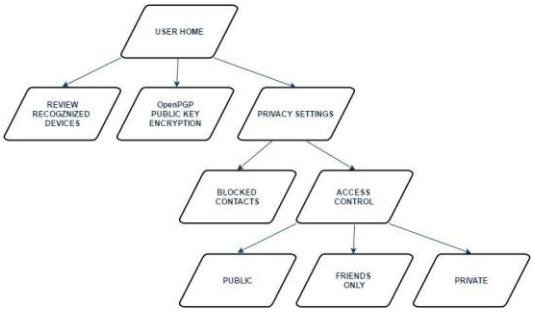

Fig. 2. Facebook Security Framework

Figure 2 shows the various security and privacy options available for a user of Facebook. Once a user logs in, Facebook checks whether the device from which the user has logged in is a recognized or not. In case the device is unrecognized, an email notification will be sent to the user's email address alerting the issue. All users also have an option of adding new or deleting existing devices. OpenPGP Public Key Encryption is used by Facebook to encrypt any email notification sent to the user by Facebook. Encryption of these notifications will ensure security and privacy of all user activity in the network. Privacy of user data and activity is an important aspect for all online social networks. Hence, Facebook has integrated a privacy settings feature in its security framework. In this feature, a user can block specific contacts and also specify the access of the user's data. The user has the freedom to restrict a particular post's access as private, friends only or public.

B. ThreatData Framework

Facebook implements a novel method known as the threat data framework to remedy the innumerous spams, scams and attacks it encounters every day. All the malicious content on Facebook is stored in classified databases, making it both a real time defensive system as well as a tool for long term analysis and research.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

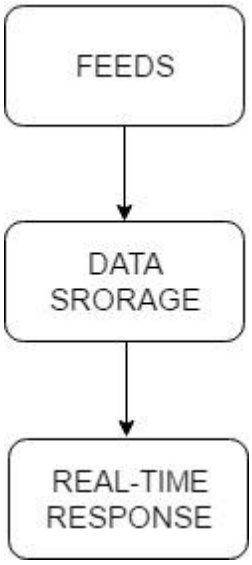

Fig. 3. Threat Data Framework

As ascertained by Facebook, the ThreatData framework is comprised of three high-level parts: feeds, data storage, and real-time response as shown in Figure 3. Feeds collect data from a specific source and are implemented via a light-weight interface. The data can be in nearly any format and is transformed by the feed into a simple schema. The datum is capable of storing not only the basics of the threat, but also the context in which it was bad. The added context is used in other parts of the framework to make more informed, automatic decisions. Once the feed has transformed the raw data, it is stored in data repositories for analysis on the prevalence and the time stamping of the threat. Both feeding and data storage are performed simultaneously with real time response, where the threat is addressed and remedied. Further, to zero down on the source of threats, all threat content is tagged with its specific geographical location. Every malicious or victimized IP address logged onto the data repository is geocoded and the corresponding frequency and spread of threat is recorded. With such efficient big data analytics implementation, cyber attackers can be easily located and penalized.

V. RESEARCH AND FUTURE IMPLEMENTATIONS

Research on how to enhance and reinforce privacy and security in social network is avid and various techniques and algorithms are proposed.

A. Trust Value Computing

Social networks such as Facebook are based on social relationships among people and they facilitate human interaction in the virtual world. These interactions include likes, comments and tags one of the most important factors of human interaction is trust [13]. Trust is the measure of confidence a user has on an entity that it will behave in an expected and stipulated behavior. Some specific properties of trust are that it is dynamic, propagative, asymmetric and context sensitive. The interactions taking place on Facebook reflect these properties. The trust between two Facebook users can keep changing over time and hence it is dynamic. Propagative trust refers to passing of information by word of mouth, creating a chain of trust and this is enforced on Facebook through the concept of "mutual friends" and "suggested friends". User A may trust user B but the reverse may not be true. Asymmetry on Facebook occurs due to difference in opinions and beliefs. Trust value computing algorithms can be used to calculate the trust value among two users on Facebook and can be used to reinforce privacy and security of the user. Many trust computing algorithms have been proposed for social networks. They usually suggest the implementation of Hybrid trust models considering both graph structures as well as interactions within the social network to calculate social trust.

- Tidal trust algorithm is a network based algorithm that uses propagative properties of trust to compute trust value. It is gradual rather than probabilistic and can be applied to the Facebook scenario by applying this to the friend selection/ friend request cases.

- Other algorithms like that of Chaverlee's and Liu's are based on individual interactions. Chaverlee's algorithm distinguishes between relationship quality and trust. It can be applied to the classification of users on Facebook based on trusted entities.

- Trust value computing may be beneficial to protect from unwanted interactions and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

classifying malicious users but it can only be implemented if the through user involvement and reporting.

B. Multimedia Data Security

The growth of multimedia sharing partnered with emerging multimedia analytic techniques like facial recognition and geo tagging has made multimedia data vulnerable to online threats. Multimedia content on Facebook, both private and social, is prone to theft, piracy and plagiarism [14]. Security of multimedia data is often taken lightly by both the users and the network administrators. A two layer security with encryption and fingerprinting or encryption and captcha is being proposed in various algorithms. . Even though this may seem cumbersome and uninviting to the viewers, it is required to enhance the security. Further, private multimedia theft can be prevented by enforcing a mechanism to notify the user when their pictures or videos are being downloaded by another user, known or unknown.

VI. CONCLUSION

Online social are vast and easy victims to cyber criminals. In this paper we have outlined the various challenges and attacks on online social networks and have provided countermeasures to deal with these attacks. We have analyzed the security framework of a popular social network to provide insight into the various methods and implementations in maintaining the security of online social networks. In the end, Social network users must be aware and be wary of online attackers and must remain prudent about the safety of their online data. Social networks are constantly expanding and so are the number of attacks and attackers. New attacks are being formulated every day and hence it is of utmost importance that we pay attention towards the safety of social networks.

REFERENCES

[1] Thelwall, M.A. (2014). "Social network sites: Users and uses". Advances in Computers.

[2] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[3] Ralph Gross and Alessandro Acquisti: Information Revelation and Privacy in Online Social Networks (The Facebook case), ACM Workshop on Privacy in the Electronic Society (WPES), 2005.

[4] Weimin Luo, Jingbo Liu, Jing Liu and Chengyu Fan: An analysis of security on social networks. Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[5] Sanaz Taheri Boshrooyeh, Alptekin Ku¨pc¸u¨ and O¨ znur O¨ zkasap: Security and Privacy of Distributed Online Social Networks, IEEE 35th International Conference on Distributed Computing Systems Workshops, 2015.

[6] Facebook: http://www.facebook.com

[7] LinkedIn: http://www.linkedin.com

[8] Twitter: http://www.twitter.com

[9] Instagram: http://www.instagram.com

[10] Sophos: https://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/facebook.aspx

[11] http://facecrooks.com/Scam-Watch/how-to-spot-a-facebook-survey-scam.html/

[12] http://www.idtheftcenter.org/

[13] Mirjam Šitum, ANALYSIS OF ALGORITHMS FOR DETERMINING TRUST AMONG FRIENDS ON SOCIAL NETWORKS, Vienna, June 2014.

[14] Mohammad H. Al Shayeji, Ghufran A. Al Shiridah, and M. D. Samrajesh: A Secure Framework for Multimedia Protection in Social Media Networks, International Journal of Innovation, Management and Technology, Vol. 3, No. 6, December 2012